Data protection & data retention in a police and national security context

International Intelligence Oversight Forum (IIOF2018):
"Latest Challenges to Intelligence Oversight in a Democracy"
Parliament Building, Valletta | 30 November 2018

Prof. Dr. Gert Vermeulen
t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be

GHENT UNIVERSITY

FACULTY OF LAW AND CRIMINOLOGY

IRCP Institute for International Research on Criminal Policy
Ghent University

PIXLES
Ghent University Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement & Surveillance

Disclosure slide | background

full-time academic

- international criminal law, EU criminal and JHA policy, cross-border judicial and police cooperation in criminal matters, mutual legal assistance (MLA)
- data protection, cybercrime, surveillance, procedural rights

data protection professional (since 2013)

- BE: Privacy commissioner, Belgian DPA (Facebook litigation, Yahoo!, Skype)
- EU: member SCG SIS II, Eurodac, VIS, CIS, Europol Cooperation Board, BTLE (Borders, Travel, Law Enforcement subgroup EDPB, preparing EDPB's opinions on the Microsoft Warrant Case and the EC's proposals on e-evidence)
- CoE: T-PD expert (Consultative Committee Convention 108+, 52 countries) for 2nd additional Protocol (e-evidence) to Budapest (Cybercrime) Convention
- ICDPPC: expert group enforcement cooperation, involved in IIOF2017

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

2 subtopics

Data retention

- introduction
- short break-out session

Cross-border e-evidence/data

- introduction
- discussion and Q&A session

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Data retention | Structure

- SIGINT debate and/versus data retention debate
- EU data protection law (applicability, relevance)
- CJEU standard setting
- data retention glass: empty or half-full?
- LE & intelligence response
- legal barriers for a plan B
- towards a Plan B?
- short break-out session

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

SIGINT debate and/versus data retention debate

important triggers in the common debate: US/Five Eyes access to bulk data

- Echelon (UKUSA agreement)
- Swift – TFTP2
- [EU-US PNR agreement]
- 2008 FISA Amendsment Act
- Snowden: Prism, Upstream etc.
- Bics & GCHQ
- etc.

mass – bulk – indiscriminate collection/retention of

- financial transaction data
- passenger data
- telecom data
- electronic communications data
- etc.

in addition to SIGINT debate (yesterday): data retention debate (this session)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

EU data protection law (applicability, relevance)

- no distinction between collection/retention or acces/use
  - both: processing
- EU compentence limited to market and criminal justice/law enforcement, including for aspects of public security (not: national security, Art. 4 TEU)
- but: EU competence to assess foreign law enforcement and state intelligence practices undermining 'adequacy' of 3rd states' data protection regimes
- blurring boundaries/purposes between criminal justice/state intelligence
- EU data retention obligations in practice transposed for both law enforcement and national security

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

CJEU standard setting

invalidating both EU & US generalised data retention practices

- 2014 Digital Rights Ireland (invalidating EU Data Retention Directive)
- 2015 Schrems v Data Protection Commissioner (invalidating Safe Harbour)
- 2016 Tele2 Sverige AB (data retention ePrivacy Directive)
- 2016 *Quadrature du Net* and Others v Commission (Privacy Shield; pending)
- Schrems III (SCC, preliminary ruling y Irish High Court; pending)
  - High Court decision October 2017: distinction mass/bulk *searching* (targeted, not indiscriminate), but involving the collection of non-relevant data, i.e. bulk *acquisition, collection or retention* = mass indiscriminate processing (Upstream)

not contradicted by

- CJEU PNR Canada Opinion (per se selective)
- ECtHR Big Brother Watch and Others v UK (no reasonable suspicion required)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Data retention glass: empty or half-full? | 1

- may not happen on a generalised basis
- may not be indiscriminate
- may not be bulk-collection
- must be limited to what is strictly necessary
- requires differentiation, limitation or exception in light of the objective pursued
- must be targeted (at least not fully untargeted; scope for 'relatively untargeted')
- must be limited to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

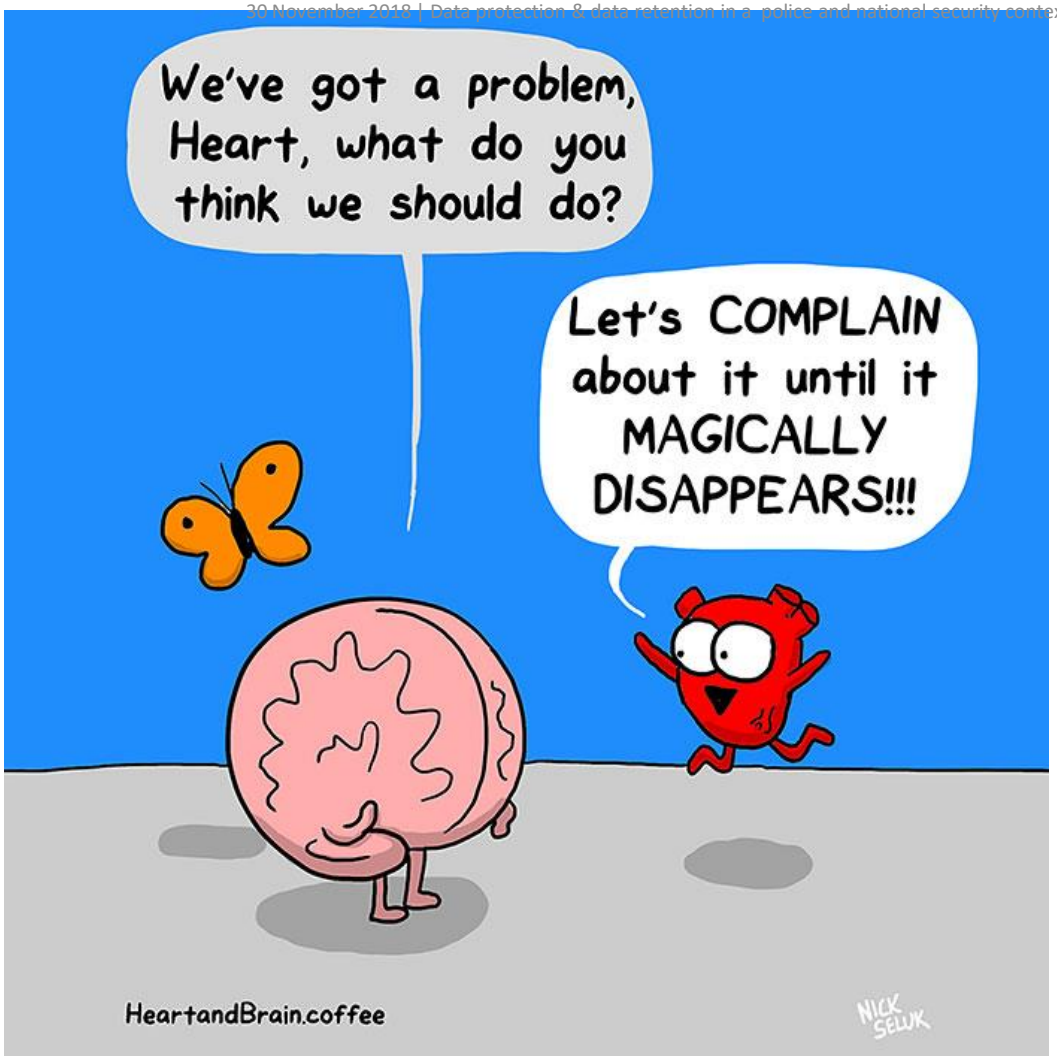
Data retention glass: empty or half-full? | 2

- must be limited with respect to (cumulatively):
  - the categories of data to be retained
  - the means of communication affected
  - the retention period adopted
  - the "persons concerned" or "the public that may potentially be affected"
- must be defined on the basis of objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security
- does not need to amount to 'reasonable suspicion', the requirement of which was dismissed in Big Brother Watch and Others v UK (ECtHR, 2018)

IRCP Institute for International Research on Criminal Policy
Ghent University

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

LE & intelligence: we want it full! | no plan at all



IRCP Institute for International Research on Criminal Policy
Ghent University

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Legal barriers for a plan B (selective retention)? | 1

relevant EU legislation

- Artt. 9 and 22 GDPR
- Att. 10-11 LED and relevant recitals (37-38)

prohibited automated processing, including profiling

- when producing adverse legal effects or significantly affecting the data subject: prohibited unless authorised by EU or MS law + appropriate safeguards, including the right to human intervention

discriminatory effects (direct or indirect)

- counter to Artt. 21 and 52 Charter

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Legal barriers for a plan B (selective retention)? | 2

use of special ('sensitive') data categories (either or not in profiling)

- processing revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
- allowed only where strictly necessary, subject to appropriate safeguards for the data subject, and only where authorised by Union or MS law
- 'appropriate safeguards': e.g. only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff, and prohibition of transmission
- example: Europol

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Legal barriers for a plan B (selective retention)? | 3

Example: Europol

- EDEN conference last week: sensitive discriminants are against HR; best way to protect against discrimination is to retain everyone's data (sic)
- whilst Europol Regulation Article 30 reads:
  - 2. Processing of [sensitive personal data], by automated or other means, shall be prohibited, unless it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol. The selection of a particular group of persons solely on the basis of such personal data shall be prohibited.
  - 3. Only Europol shall have direct access to personal data as referred to in paragraphs 1 and 2. The Executive Director shall duly authorise a limited number of Europol officials to have such access if it is necessary for the performance of their tasks.
  - 4. No decision by a competent authority which produces adverse legal effects concerning a data subject shall be based solely on automated processing of data as referred to in paragraph 2, unless the decision is expressly authorised pursuant to national or Union legislation.

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Plan B | Checklist: evidence, feasible, lawful?

irrespective of

- selectors/discriminants used
- type of info the retention is envisaged of (subscriber data, access data, transactional data, geo-location data, content data, …)

check

- evidence base? (objective or objectifiable)
  - police/intelligence databases
  - conviction databases
  - strategic analysis insights
  - …
- feasibility of implementation? (technical, operational, financial, …)
- use of sensitive data (profiling)? (requiring an explicit legal basis and appropriate, suitable safeguards)
- discriminatory effect? (direct or indirect?)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Plan B | Possible selectors or discriminants

ratione personae (characteristics of targeted persons)

- age, gender, nationality, racial or ethnic origin, political opinion, religious or philosophical beliefs, membership (of an association, trade union, …), …

ratione loci (residence or presence of targeted persons)

- city, street, neighbourhood, public space, square, …

ratione itineris (targeted routes of communications or data flows, in terms of origin, transit, destination or combinations thereof)

- country/city, neighbourhood/building, server, company, hotspot, provider, geo-location pattern (e.g. BE wifi sniffer proposal to combat smuggling) …

ratione temporis (targeted period or time frame(s); duration pattern)

- month/week/day/time-slot, event-based (concert, Xmas market, football match, …), suspicious timings, ringing pattern

ratione instrumenti (targeting persons using certain means of communication)

- use(rs) of certain communication means (Signal, Telegram, …), encryption tools, secure VPN's, …, foreign (unregistered) sim cards (roaming), …

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Break-out session

explorative, interactive, constructive exercise

reporting back (volunteer spokespersons)

IRCP Institute for International Research on Criminal Policy
Ghent University

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Cross-border acces to e-evidence/data | Structure

jurisdiction and e-evidence: the issue

cross-jurisdictional e-evidence

- Europe
- EU-US

cases and clashes

- Google Spain; Microsoft Warrant; Facebook, Yahoo! & Skype

proposed solutions

- EU level
- CoE level
- [PM: global level: UN special rapporteur | international data access warrant]

competing, legitimate interests at stake

fundamental rights considerations & concerns

discussion and Q&A session

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Jurisdiction & e-evidence | the issue

- criminal justice authorities: tradition of cross-border access/MLA based on jurisdictional rules and territory-/sovereignty-based controls and limitations
- unique features of electronic data: increasingly extraterritorial effect
- loss of location (data moving between different services, providers, locations and jurisdictions): what is territorial and what is extraterritorial?
  - possible conflicts of law
  - complexity/fragmentation
  - legal uncertainty for both public authorities and private service providers
  - countries hosting major service providers/data centres: ever-increasing number of requests for e-evidence
- jurisdictional questions often determine the rights and protections that apply (in particular (EU) privacy regulations; GDPR, LED)
- private parties that hold and manage our data increasingly determine whose rules govern and, in key ways, how they are interpreted and applied
  - note: inclusive of so called Over-The-Top (OTT) services, as they are functionally equivalent to more traditional electronic or telecommunication services

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Cross-jurisdictional e-evidence | Europe

current frameworks

- domestic
  - cooperation obligation for telecom and electronic communication providers
  - initially in criminal matters, soon extended to national security matters
- bilateral and multilateral
  - mutual legal assistance (MLA) instruments
  - Budapest Convention, European Investigation Order, …

cross-border access

- formal cooperation between relevant authorities (MLA/EIO) or police-to-police cooperation (or intelligence service infoex)
- direct cooperation between judicial/law enforcement authority and service provider in another country (voluntary/mandatory) | likely soon extended to national security purposes/intelligence services
- direct access from computer

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Cross-jurisdictional e-evidence | EU-US

- Electronic Communications Privacy Act (ECPA) | Stored Communications Act (SCA)
- CLOUD Act (Clarifying Lawful Overseas Use of Data)
  - amendment to the SCA to require service providers to "preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."
  - "qualifying" foreign governments get access to records stored in the U.S. that pertain to foreign citizens
- criticism
  - proper safeguards for consumer privacy?
    - discriminatory application to foreign citizens living in the U.S.
    - lack of notice provisions
    - omission of any requirement to obtain a warrant
  - effect on the existing MLA procedures?
  - *quid* GDPR which prohibits the transfer or disclosure of personal data unless pursuant to an MLAT or other international agreement?
  - trans-Atlantic agreement needed

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Cases & clashes

Google Spain case (no primacy of location HQ or data processing)

- EU Court of Justice (13/05/'14): processing of personal data by Google Search is carried out 'in the context of the activities of the establishment in Spain'

Facebook Belgium case (idem)

- BE competence to enforce domestic privacy laws relating to processing of personal data by FB Ireland (on behalf on FB Inc), since carried out in the context of the activities of an establishment on BE territory of the controller (FB Belgium)

Yahoo! Belgium case (primacy of data access over data location) (subscriber information)

- territoriality determined by where data is accessed/received, not where it is located

Skype Belgium case (idem, also for content; lack of office/establishment irrelevant)

- Skype (LU-based) subject to BE jurisdiction by actively participating in the economic life a.o. by language-adapted adverstisment and can be compelled to locally cooperate

Microsoft Warrant case (EU data location-based complication)

- 2nd circuit court '16): law enforcement needs to make an MLA request to foreign government where data is located (Ireland); even so if the crime, victim and target of the investigation are all located in the U.S.
- Supreme Court '18: case declared 'moot' against the backdrop of the Cloud Act

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Proposed solutions | EU level

2016 Council conclusions on criminal justice in cyberspace – Final report

practical measures : improving cooperation

- among judicial authorities
  - within the EU: electronic user-friendly EIO; platform for digital exchanges
  - with the US: dialogue; exchange of best practice; training; information platform
- with service providers (*de facto* main channel),
  e.g. SPOC's, streamlining policies, standardising/reducing forms used in MS

legislative measures (April 2018: 2 EC proposals; MLA "too cumbersome")

- proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters
- proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings
- several issues with legal basis
- more fundamental: judicial cooperation/MLA substituted with compulsory public-private cooperation

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Proposed solutions | CoE level

Budapest (Cybercrime) Convention

- guidance note to accompany art. 18 (production order for subscriber information)
  - requirement mechanism by which law enforcement officials can order "a person in its territory to submit computer data in that person's possession or control"
  - broad jurisdictional reach over extraterritorial providers, without disclaiming government efforts to block such foreign government reach
- initiation draft 2nd additional protocol regarding
  - provisions for more effective MLA (facilitating access to data in foreign, multiple and unknown jurisdictions)
  - provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information (inclusive of dynamic IP addresses?), preservation requests, and emergency requests
  - clearer framework and stronger safeguards (including data protection requirements, as resulting from Convention 108+) for existing practices of trans-border data access

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Competing, legitimate interests/rights at stake

<u>of states</u>

- right to compell service providers (including OTT) to cooperate re the use of services offered on their territory (i.e. when having an establishment, office or other substantial connection)
- sovereignty of the territory & territoriality of criminal law (clashes; MLA)

<u>of the data subject/person concerned</u>

- right to privacy and data protection
- procedural rights protection

<u>of private companies</u>

- freedom of establishment; right to conduct business/offer services in a global market
- legitimate business interest
- should not be attributed a formal role
  - on behalf of states (in checking whether conditions in requesting/issuing state are fulfilled, whether there are immunities, let alone whether there is sufficient prima facie evidence, …)
  - nor on behalf of the data subject/person concerned (too strongly data location-based interpretation)

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Fundamental rights considerations & concerns

proportionality should be assessed based on the intrusiveness of the data type

- subscriber data (inclusive of dynamic IP addresses) (CoE) or subriber and access data (EU): no offence threshold, can be ordered by prosecutor (no judge required)
- traffic and content data (CoE) or transactional and content data: offence threshold & court/judge production order (preservation order: prosecutor)

data and procedural protection must – again – be maximised (as in MLA)

- in times of 'loss of location', the data storage location (even if relevant from a data protection perspective, especially to shield EU data from US surveillance) seems the least relevant criterion to govern the data protection and procedural rights safeguards that should apply
- work with the combined data protection and procedural rights obligations (double *locus* regime, not just double criminality) of at least
  - as far as subscriber or access data are concerned (or, for mere preservation purposes, of transactional or content data): the country of the requesting/issuing competent authority and the country where the service provider is located
  - as far as transactional or content data are concerned: the country of the requesting/issuing competent authority and the country where the data subject was present whilst using the targeted service (which will be known based on the subscriber/access data)
  - thus putting a person's legitimate expectation of privacy back at the forefront

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

Discussion | Q&A

IRCP Institute for International Research on Criminal Policy
Ghent University

Prof. Dr. Gert Vermeulen
+32 9 264 69 43
Gert.Vermeulen@UGent.be

www.ircp.org

Contact

Prof. Dr. Gert Vermeulen

t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be

http://www.linkedin.com/in/gert-vermeulen-42b00068

IRCP

Ghent University
Universiteitstraat 4
B – 9000 Ghent

GHENT UNIVERSITY

FACULTY OF LAW AND CRIMINOLOGY

IRCP Institute for International Research on Criminal Policy
Ghent University

PIXLES
Ghent University Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement & Surveillance